#2

Attorney Docket No. 1504.1006

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**


In re Patent Application of:

Shigeichiro YAMASAKI, et al.

Application No.: Group Art Unit:

Filed: September 24, 2001 Examiner:

For: CONTENT DISTRIBUTION SYSTEM

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-129485

Filed: April 26, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 24, 2001 By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

# 日 本 国 特 許 庁
# JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ４月２６日

出願番号
Application Number: 特願２００１－１２９４８５

出願人
Applicant(s): 富士通株式会社



２００１年 ７月 ６日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

【書類名】　特許願

【整理番号】　0195029

【提出日】　平成13年 4月26日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

H04L 9/00

【発明の名称】　コンテント配信システム、耐タンパ装置、サーバ、コンピュータ・プログラム、およびコンテント配信方法

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　山崎　重一郎

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　塩内　正利

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　岩尾　忠重

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　和田　裕二

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　岡田　誠

【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100086380
【弁理士】
【氏名又は名称】　吉田　稔
【選任した代理人】
【識別番号】　100103078
【弁理士】
【氏名又は名称】　田中　達也
【選任した代理人】
【識別番号】　100105832
【弁理士】
【氏名又は名称】　福元　義和
【連絡先】　０６－６７６４－６６６４
【手数料の表示】
【予納台帳番号】　024198
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9807281
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテント配信システム、耐タンパ装置、サーバ、コンピュータ・プログラム、およびコンテント配信方法

【特許請求の範囲】

【請求項１】　配信者からコンテントの配信を受ける利用者のデータ処理装置と、

配信者と利用者との双方から信任された第三者機関のデータ処理装置と、

前記各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムであって、

前記利用者のデータ処理装置は、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置を備えており、

前記第三者機関のデータ処理装置は、前記配信者によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、前記耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを前記利用者のデータ処理装置に送信し、

前記耐タンパ装置は、前記第三者機関のデータ処理装置からの前記第１のデータを用いて、前記暗号化されたコンテントを復号化する構成としたことを特徴とする、コンテント配信システム。

【請求項２】　コンテントを配信する配信者のデータ処理装置と、

コンテントの配信を受ける利用者のデータ処理装置と、

配信者と利用者との双方から信任された第三者機関のデータ処理装置と、

前記各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムであって、

前記配信者のデータ処理装置は、コンンツを暗号化して前記利用者のデータ処理装置に配信し、

前記利用者のデータ処理装置は、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置を備えており、

前記第三者機関のデータ処理装置は、前記暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、前記耐タンパ装置の内部でのみ暗号鍵

を求め得る第１のデータを前記利用者のデータ処理装置に送信し、

前記耐タンパ装置は、前記第三者機関のデータ処理装置からの前記第１のデータを用いて、前記暗号化されたコンテントを復号化する構成としたことを特徴とする、コンテント配信システム。

【請求項３】　前記第三者機関のデータ処理装置は、公開鍵と秘密鍵とを記憶しており、前記配信者のデータ処理装置からの要求に応じて前記公開鍵を前記配信者のデータ処理装置に送信し、

前記配信者のデータ処理装置は、前記第三者機関のデータ処理装置から受信した前記公開鍵を用いて前記暗号鍵を暗号化し、その暗号化された暗号鍵を前記利用者のデータ処理装置に送信し、

前記利用者のデータ処理装置は、前記配信者のデータ処理装置から受信した前記暗号化された暗号鍵に基づく第２のデータを前記耐タンパ装置に生成させ、その第２のデータを前記第三者機関のデータ処理装置に送信し、

前記第三者機関のデータ処理装置は、前記利用者のデータ処理装置から受信した前記第２のデータと前記秘密鍵とを用いて前記第１のデータを生成する、請求項２に記載のコンテント配信システム。

【請求項４】　前記第三者機関は、複数存在し、

前記耐タンパ装置は、前記第２のデータを、前記暗号鍵が解読されないように秘密分散させて前記各第三者機関毎に各別に生成し、前記複数の第三者機関によって各別に生成された複数の前記第１のデータを用いて前記暗号鍵を解読し、その暗号鍵を用いて前記暗号化されたコンテントを復号化する、請求項３に記載のコンテント配信システム。

【請求項５】　前記耐タンパ装置は、前記暗号化された暗号鍵から前記第２のデータを生成するに際して、乱数成分を混入させ、前記第１のデータを用いて前記暗号化されたコンテントを復号化するに際して、前記第１のデータから前記乱数成分を除去する、請求項３または４に記載のコンテント配信システム。

【請求項６】　前記耐タンパ装置は、前記公開鍵に関する情報を、認証機関によるデジタル証明書の形式で記憶しており、かつ、前記認証機関により本人確認の上で各利用者に配布され、

前記第三者機関のデータ処理装置は、前記利用者のデータ処理装置から前記デジタル証明書の形式の前記公開鍵に関する情報を受信することにより、利用者の確認を行う、請求項２ないし５のいずれかに記載のコンテント配信システム。

【請求項７】　コンテントを配信する配信者のデータ処理装置と、前記コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、前記各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムにおいて、前記利用者のデータ処理装置に備えられ、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置であって、

前記第三者機関のデータ処理装置から受信した、前記配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵に関するデータを用いて、前記暗号鍵を解読する解読手段と、

前記解読手段によって解読された前記暗号鍵を用いて前記暗号化されたコンテントを復号化する復号化手段とを備えたことを特徴とする、耐タンパ装置。

【請求項８】　コンテントを配信する配信者のデータ処理装置と、前記コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、前記各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムにおいて、前記第三者機関のデータ処理装置を実現するサーバであって、

前記配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、前記利用者のデータ処理装置に備えられた外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを生成するデータ生成手段と、

前記データ生成手段によって生成された前記第１のデータを前記通信網を介して前記利用者のデータ処理装置に送信するデータ送信手段とを備えたことを特徴とする、サーバ。

【請求項９】　コンテントを配信する配信者のデータ処理装置と、前記コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、前記各データ処理装置を相互に通信

可能に接続する通信網とを有するコンテント配信システムにおいて、前記第三者機関のデータ処理装置を動作させるためのコンピュータ・プログラムであって、

前記配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、前記利用者のデータ処理装置に備えられた外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを生成するためのデータ生成プログラムと、

前記データ生成プログラムによって生成された前記第１のデータを前記通信網を介して前記利用者のデータ処理装置に送信するためのデータ送信プログラムとを含むことを特徴とする、コンピュータ・プログラム。

【請求項１０】　配信者から暗号化されたコンテントの配信を受ける利用者のデータ処理装置と、

配信者と利用者との双方から信任された第三者機関のデータ処理装置と、

前記各データ処理装置を相互に通信可能に接続する通信網とを有するシステムにおいて実行されるコンテント配信方法であって、

前記利用者のデータ処理装置が、前記第三者機関のデータ処理装置に対して前記コンテントに対する支払い手続を指示するステップと、

前記第三者機関のデータ処理装置が、前記コンテントの対価について利用者の口座から第三者機関の口座への振替または振込が成功したときに、前記利用者のデータ処理装置でのみ暗号鍵を求め得る第１のデータを前記利用者のデータ処理装置に送信するステップと、

前記利用者のデータ処理装置が、前記第三者機関のデータ処理装置からの前記第１のデータを用いて、前記暗号化されたコンテントを復号化するステップと、

を含むことを特徴とする、コンテント配信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インターネットなどの通信網や光ディスクなどの記憶媒体を利用した、音楽や映像やソフトウェアなどのデジタル著作物（以下「コンテント」と記す）を配信するための、コンテント配信システム、耐タンパ装置、サーバ、およ

びコンピュータ・プログラムに関する。

【０００２】

【従来の技術】

著作権者あるいはその依頼を受けた仲介業者などの配信者がコンテントを暗号化して配信するシステムでは、正当な対価を支払った利用者のみが暗号化されたコンテントを復号化できるようにするために、安全な暗号鍵の配布手段が必要となる。

【０００３】

特に、個人や小規模の事業者が配信者としてコンテントを配布する場合や、オークションによるコンテントの取引や、現在増加しつつある、サーバを利用せずに端末システムから端末システムへの複製の連鎖を利用したＰ２Ｐ(peer to peer)と呼ばれる形態でのコンテント配信において、配信者と利用者とが安全に対価の支払いと暗号鍵の受け渡しとを行うには、配信者と利用者との双方から信用され決済機能を持つ第三者機関によるいわゆるライセンス鍵のエスクロー(escrow)サービスが必要となる。

【０００４】

【発明が解決しようとする課題】

しかし、従来のライセンス鍵を購入者に渡す方法によるエスクローサービスでは、利用者に直接コンテントを復号化できる暗号鍵が渡されるために、暗号鍵を取得した利用者がその暗号鍵を再配布することによる不正を防ぐことができなかった。

【０００５】

【発明の開示】

本発明は、上記した事情のもとで考え出されたものであって、暗号鍵を確実に秘匿できるコンテント配信システム、およびそれに用いる耐タンパ装置、サーバ、ならびにコンピュータ・プログラムを提供することを、その目的とする。

【０００６】

上記課題を解決するため、本発明では、次の技術的手段を講じている。

【０００７】

本発明の第１の側面によれば、配信者からコンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムであって、利用者のデータ処理装置は、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置を備えており、第三者機関のデータ処理装置は、配信者によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを利用者のデータ処理装置に送信し、耐タンパ装置は、第三者機関のデータ処理装置からの第１のデータを用いて、暗号化されたコンテントを復号化する構成としたことを特徴とする、コンテント配信システムが提供される。

【０００８】

本発明の第２の側面によれば、コンテントを配信する配信者のデータ処理装置と、コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムであって、配信者のデータ処理装置は、コンンツを暗号化して利用者のデータ処理装置に配信し、利用者のデータ処理装置は、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置を備えており、第三者機関のデータ処理装置は、暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを利用者のデータ処理装置に送信し、耐タンパ装置は、第三者機関のデータ処理装置からの第１のデータを用いて、暗号化されたコンテントを復号化する構成としたことを特徴とする、コンテント配信システムが提供される。

【０００９】

好ましい実施の形態によれば、第三者機関のデータ処理装置は、公開鍵と秘密鍵とを記憶しており、配信者のデータ処理装置からの要求に応じて公開鍵を配信者のデータ処理装置に送信し、配信者のデータ処理装置は、第三者機関のデータ処理装置から受信した公開鍵を用いて暗号鍵を暗号化し、その暗号化された暗号鍵を利用者のデータ処理装置に送信し、利用者のデータ処理装置は、配信者のデ

ータ処理装置から受信した暗号化された暗号鍵に基づく第２のデータを耐タンパ装置に生成させ、その第２のデータを第三者機関のデータ処理装置に送信し、第三者機関のデータ処理装置は、利用者のデータ処理装置から受信した第２のデータと秘密鍵とを用いて第１のデータを生成する。

【００１０】

他の好ましい実施の形態によれば、第三者機関は、複数存在し、耐タンパ装置は、第２のデータを、暗号鍵が解読されないように秘密分散させて各第三者機関毎に各別に生成し、複数の第三者機関によって各別に生成された複数の第１のデータを用いて暗号鍵を解読し、その暗号鍵を用いて暗号化されたコンテントを復号化する。

【００１１】

他の好ましい実施の形態によれば、耐タンパ装置は、暗号化された暗号鍵から第２のデータを生成するに際して、乱数成分を混入させ、第１のデータを用いて暗号化されたコンテントを復号化するに際して、第１のデータから乱数成分を除去する。

【００１２】

他の好ましい実施の形態によれば、耐タンパ装置は、公開鍵に関する情報を、認証機関によるデジタル証明書の形式で記憶しており、かつ、認証機関により本人確認の上で各利用者に配布され、第三者機関のデータ処理装置は、利用者のデータ処理装置からデジタル証明書の形式の公開鍵に関する情報を受信することにより、利用者の確認を行う。

【００１３】

本発明の第３の側面によれば、コンテントを配信する配信者のデータ処理装置と、コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムにおいて、利用者のデータ処理装置に備えられ、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置であって、第三者機関のデータ処理装置から受信した、配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵

に関するデータを用いて、暗号鍵を解読する解読手段と、解読手段によって解読された暗号鍵を用いて暗号化されたコンテントを復号化する復号化手段とを備えたことを特徴とする、耐タンパ装置が提供される。

【００１４】

本発明の第４の側面によれば、コンテントを配信する配信者のデータ処理装置と、コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムにおいて、第三者機関のデータ処理装置を実現するサーバであって、配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、利用者のデータ処理装置に備えられた外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを生成するデータ生成手段と、データ生成手段によって生成された第１のデータを通信網を介して利用者のデータ処理装置に送信するデータ送信手段とを備えたことを特徴とする、サーバが提供される。

【００１５】

本発明の第５の側面によれば、コンテントを配信する配信者のデータ処理装置と、コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムにおいて、第三者機関のデータ処理装置を動作させるためのコンピュータ・プログラムであって、配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、利用者のデータ処理装置に備えられた外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを生成するためのデータ生成プログラムと、データ生成プログラムによって生成された第１のデータを通信網を介して利用者のデータ処理装置に送信するためのデータ送信プログラムとを含むことを特徴とする、コンピュータ・プログラムが提供される。

【００１６】

本発明の第６の側面によれば、配信者から暗号化されたコンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、各データ処理装置を相互に通信可能に接続する通信網とを有するシステムにおいて実行されるコンテント配信方法であって、利用者のデータ処理装置が、第三者機関のデータ処理装置に対してコンテントに対する支払い手続を指示するステップと、第三者機関のデータ処理装置が、コンテントの対価について利用者の口座から第三者機関の口座への振替または振込が成功したときに、利用者のデータ処理装置でのみ暗号鍵を求め得る第１のデータを利用者のデータ処理装置に送信するステップと、利用者のデータ処理装置が、第三者機関のデータ処理装置からの第１のデータを用いて、暗号化されたコンテントを復号化するステップと、を含むことを特徴とする、コンテント配信方法が提供される。

【００１７】

本発明によれば、第三者機関のデータ処理装置が、配信者によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを利用者のデータ処理装置に送信し、耐タンパ装置が、第三者機関のデータ処理装置からの第１のデータを用いて、暗号化されたコンテントを復号化するので、耐タンパ装置の外部からは暗号鍵を知ることができず、暗号鍵を確実に秘匿できる。

【００１８】

本発明のその他の特徴および利点については、以下に行う発明の実施の形態の説明から、より明らかになるであろう。

【００１９】

【発明の実施の形態】

以下、本発明の好ましい実施の形態について、図面を参照して具体的に説明する。

【００２０】

図１は、本発明に係るコンテント配信システムの概略構成図である。このコンテント配信システムは、利用者の端末装置１、第三者機関のサーバ２、著作権者

の端末装置３、および通信網４を備えている。利用者の端末装置１および著作権者の端末装置３は、多数の利用者や多数の著作権者に対応してそれぞれ多数存在している。通信網４は、たとえばインターネット、インターネットの接続サービス事業者のサーバ、通信事業者の公衆回線網、社内ＬＡＮ（local area network）などを全て含んでいる。すなわち、利用者の端末装置１と第三者機関のサーバ２と著作権者の端末装置３とは、その具体的な通信ルートを問わず、通信網４を介して相互にデータ通信可能であればよい。

【００２１】

図２は、利用者の端末装置１の要部の構成図である。利用者の端末装置１は、コンテント再生処理部１１、および記憶部１２を備えており、耐タンパデバイス１３を着脱可能である。耐タンパデバイス１３は、演算部２１、乱数生成部２２、復号化部２３、一時記憶部２４、および長期記憶部２５を備えている。

【００２２】

図３は、本発明に係るコンテント配信システムにおける配信プロトコルの説明図である。図３において、認証機関５は、利用者に本人確認のうえで耐タンパデバイス１３を発行する。

【００２３】

利用者の端末装置１は、たとえばパーソナルコンピュータにより実現されている。もちろん利用者の端末装置１は、携帯型電話装置などを含む各種モバイル装置、データ通信機能を有する家庭用ゲーム装置、あるいはデータ処理機能を有するテレビジョン受像機などの各種の家電装置であってもよい。

【００２４】

コンテント再生処理部１１は、著作権者の端末装置３から配信されて記憶部１２に格納された、暗号化されたコンテントを再生する。この再生に際しては、暗号化されたコンテントを復号化するために、耐タンパデバイス１３内の暗号系を利用する。このコンテント再生処理部１１は、利用者の端末装置１に内蔵されたＣＰＵ（central processing unit）により実現される。

【００２５】

記憶部１２には、著作権者の端末装置３から配信されたコンテントが格納され

る。このコンテントは、暗号化されている。記憶部１２は、たとえばハードディスク装置により実現される。もちろん記憶部１２として、書き替え可能な不揮発性メモリ、電源バックアップの施された揮発性メモリ、あるいは各種光ディスクなどを用いてもよい。

【００２６】

耐タンパデバイス１３は、各利用者毎に、信頼できる認証機関５から発行されたデバイスであって、利用者以外の者はもちろんのこと、利用者自身も内部のデータを知ることができない。この耐タンパデバイス１３は、たとえばＩＣカードによって実現されている。

【００２７】

演算部２１は、たとえば１０２４ビット程度の巨大な整数のべき剰余計算機能を有している。また演算部２１は、第三者機関のサーバ２からのデータに基づいて、著作権者の端末装置３がコンテントを暗号化したのと同じアルゴリズムによる復号化のための暗号鍵を演算し、それを一時記憶部２４に格納する。

【００２８】

乱数生成部２２は、乱数を生成する。

【００２９】

復号化部２３は、演算部２１によって演算された暗号鍵を用いて、記憶部１２に格納されている暗号化されたコンテントを復号化する。

【００３０】

一時記憶部２４は、乱数生成部２２によって生成された乱数を記憶する。この一時記憶部２４は、たとえばレジスタあるいはＲＡＭ（random access memory）によって実現されている。

【００３１】

長期記憶部２５には、個々の利用者固有の、換言すれば個々の耐タンパデバイス１３固有の公開鍵暗号に基づく秘密鍵とそれに対応する公開鍵とが、認証機関５によって署名されたデジタル証明書の形で格納されている。

【００３２】

第三者機関のサーバ２は、著作権者と利用者との双方が信頼することが可能な

第三者機関（以下、「エスクロー機関」と記すこともある）の運営するサーバであって、以下の機能を有している。すなわち、公開鍵暗号に基づいた第三者機関固有の秘密鍵と公開鍵とを有し、デジタル証明書などの安全な方法で著作権者に自己の公開鍵を配布する。また、耐タンパデバイス１３の発行元である認証機関５のデジタル証明書の電子署名の検証によって、利用者の耐タンパデバイス１３の長期記憶部２５に格納されている公開鍵の正真性を検証する。また、たとえば１０２４ビット程度の巨大な整数のべき剰余計算を行う。また、自身が発行する公開鍵証明書に、第三者機関のサーバ２へのアクセス方法などの情報を記載する。第三者機関は、たとえば銀行などの金融業者あるいはその提携企業などである。

【００３３】

配信者としての著作権者の端末装置３は、共通鍵暗号に基づく暗号化機能を備えており、コンテントを暗号鍵で暗号化し、その暗号化コンテントを利用者の端末装置１に配信する。コンテントを暗号化するための暗号鍵は、著作権者が自己の端末装置３を用いて生成し、他者に漏洩しないように安全に管理する。本実施形態においては、著作権者は、信頼できる第三者機関に決済口座を持っているものとする。もちろん著作権者の端末装置３は、携帯型電話装置などを含む各種モバイル装置、データ通信機能を有する家庭用ゲーム装置、あるいはデータ処理機能を有するテレビジョン受像機などの各種の家電装置であってもよい。

【００３４】

認証機関５は、耐タンパデバイス１３とその所持者との対応関係を保証する信頼できる機関であり、耐タンパデバイス１３の長期記憶部２５に安全に格納されている秘密鍵と対になる公開鍵に対して公開鍵証明書の形で電子署名を行う。

【００３５】

次に動作を説明する。

【００３６】

先ず著作権者が、端末装置３を使用することにより、自己のコンテントＣに対して、自ら生成したライセンスキーとなる暗号鍵Ｋを使って暗号化を行い、暗号化コンテントＫ（ｃ）を生成する。また著作権者は、端末装置３を使用すること

により、第三者機関のサーバ２から第三者機関の公開鍵＜ｅ，ｎ＞を安全な公開鍵証明書の形で入手し、公開鍵証明書の公開鍵＜ｅ，ｎ＞を用いて、ライセンスキーとなる暗号鍵ＫをＫ$^{e}$ mod(n)として暗号化する。ただし、Ｋとｎとは互いに素な整数である。また、Ｋ$^{e}$ mod(n)は、Ｋのｅ乗をｎで除した場合の剰余である。そして著作権者は、端末装置３を利用して、暗号化コンテントＫ（ｃ）と、暗号化されたライセンス鍵Ｋ$^{e}$ mod(n)と、第三者機関の公開鍵証明書とを一体化したもの、すなわち＜Ｋ（ｃ），Ｋ$^{e}$ mod(n)，＜ｅ，ｎ＞＞を、利用者の端末装置１に配信する。

【００３７】

著作権者の端末装置３から＜Ｋ（ｃ），Ｋ$^{e}$ mod(n)，＜ｅ，ｎ＞＞を受け取った利用者は、そのコンテントＣの再生を希望する場合、利用者の端末装置１の記憶部１２に暗号化コンテントＫ（ｃ）を格納するとともに、暗号化されたライセンス鍵Ｋ$^{e}$ mod(n)と、第三者機関の公開鍵＜ｅ，ｎ＞とを耐タンパデバイス１３に入力する。

【００３８】

これにより耐タンパデバイス１３の乱数生成部２２が、乱数ｒを生成し、その乱数ｒを一時記憶部２４に記憶させる。そして演算部２１が、（Ｋ$^{e}$ ｒ$^{e}$）mod(n)を演算する。この操作によって、乱数成分が加わるために、ライセンスキーとしての暗号鍵Ｋが匿名化される。ただし、乱数ｒはｎと互いに素な整数を選択するものとする。さらに演算部２１が、長期記憶部２５に記憶されている秘密鍵ｄＵを用いて、（（Ｋ$^{e}$ ｒ$^{e}$）mod(n)）$^{dU}$mod(nU) を演算する。これは、第三者機関に耐タンパデバイス１３が秘密鍵ｄＵを所持していることを証明するために利用される。そして耐タンパデバイス１３が、暗号化コンテントＫ（ｃ）に添付されている第三者機関の公開鍵証明書に記載されているアクセス情報に基づいて、第三者機関のサーバ２に＜（（Ｋ$^{e}$ ｒ$^{e}$）mod(n)）$^{dU}$mod(nU)，（Ｋ$^{e}$ mod(n)）（ｒ$^{e}$ mod(n)）＞を送信する。

【００３９】

利用者の端末装置１から＜（（Ｋ$^{e}$ ｒ$^{e}$）mod(n)）$^{dU}$mod(nU)，（Ｋ$^{e}$ mod(n)）（ｒ$^{e}$ mod(n)）＞を受信した第三者機関のサーバ２は、先ず、利用者の公開鍵

証明書に付与されている認証機関の電子署名を検証することによって、利用者の公開鍵＜ｅＵ，ｎＵ＞の正当性を調べる。利用者の公開鍵＜ｅＵ，ｎＵ＞の正当性が証明されると、第三者機関のサーバ２は、利用者の端末装置１から受信した＜（（$K^e$ $r^e$）mod(n)）$^{dU}$mod(nU)，（$K^e$ mod(n)）（$r^e$ mod(n)）＞に基づいて、利用者の認証を行う。すなわち第三者機関のサーバ２が、（（$K^e$ $r^e$）mod(n)）$^{dU}$mod(nU) を用いて、（（$K^e$ $r^e$）mod(n)）$^{dU}$mod(nU) ＝（$K^e$ $r^e$）mod(n)を演算し、これと（$K^e$ mod(n)）（$r^e$ mod(n)）とを比較して、一致していれば、送信者が正当な使用者であると認証する。すなわち、このような暗号化ができるのは、公開鍵＜ｅＵ，ｎＵ＞に対応する秘密鍵ｄＵを内蔵する耐タンパデバイス１３のみであるので、このデータの送信者が正当な利用者であると判断できる。また、このときに、通常のライセンスキーの購入と同等の手続きによって、利用者は第三者機関にコンテントの対価を支払う。この第三者機関は、決済のエスクロー機関としての役割に基づき、著作権者への決済口座への振込みを、利用者からの受け取り確認を得るまで遅延させる。

【００４０】

次に第三者機関のサーバ２は、自己の秘密鍵ｄを用いて、利用者の端末装置１から受け取った情報を（$K^e$ $r^e$）$^d$ mod(n)＝（Ｋｒ）mod(n)によって復号化する。すなわち、第三者機関の公開鍵＜ｅ，ｎ＞および秘密鍵ｄは、オイラーの定理により上記の等式を満足するように決定されている。この計算結果には、乱数成分ｒが乗じられており、一般に巨大な整数の素因数分解は非常に困難であるために、この値から暗号鍵Ｋを見つけることは、事実上不可能である。そして第三者機関のサーバ２は、（Ｋｒ）mod(n)を利用者の端末装置１に送信する。

【００４１】

第三者機関のサーバ２から（Ｋｒ）mod(n)を受信した利用者の端末装置１は、それを耐タンパデバイス１３に供給する。これにより耐タンパデバイス１３の演算部２１は、一時記憶部２４に記憶している乱数ｒを用いてｒmod(n)の逆数すなわち$r^{-1}$mod(n)を演算し、その演算結果と（Ｋｒ）mod(n)とを乗算することによって暗号鍵Ｋを演算し、一時記憶部２４に格納する。mod(n)におけるｎと素な整数の逆数は、互除法などの効率的なアルゴリズムを用いて演算できる。

【００４２】

そしてコンテント再生処理部１１が、コンテントＣを再生する。すなわち、コンテント再生処理部１１が、記憶部１２から読み出した暗号化コンテントＫ（ｃ）を耐タンパデバイス１３に供給する。これにより耐タンパデバイス１３の復号化部２３が、一時記憶部２４に記憶されている暗号鍵Ｋを用いて、暗号化コンテントＫ（ｃ）を復号化し、それをコンテント再生処理部１１に供給する。コンテント再生処理部１１は、復号化部２３により復号化されたコンテントＣを再生し、利用者の端末装置１の表示部（図示せず）などに出力する。このような処理は、再生終了まで順次継続される。このように、暗号鍵Ｋを耐タンパデバイス１３の外部に取り出すこと無く、その暗号鍵Ｋに基づく固有の計算能力のみを利用して復号化を行うことによって、暗号鍵Ｋを利用者が再配布することを防止している。

【００４３】

図４は、コンテンツ配信に伴う利用料金の決済の一例を説明する説明図である。

【００４４】

先ず、エスクロー機関すなわち第三者機関が売り手すなわち配信者に公開鍵を渡す。具体的には、第三者機関のサーバ２が著作権者の端末装置３に公開鍵＜ｅ，ｎ＞を送信する。

【００４５】

そして、売り手が買い手すなわち利用者にコンテンツＣを配信する。具体的には、著作権者の端末装置３が、暗号化コンテンツＫ（ｃ）と暗号化されたライセンスキーすなわち暗号鍵$K^{e} \bmod(n)$とを利用者の端末装置１に配信する。

【００４６】

配信を受けた買い手は、エスクロー機関に支払い手続を行う。具体的には、利用者の端末装置１が、＜（（$K^{e} r^{e}$）$\bmod(n)$）$^{dU} \bmod(nU)$，（$K^{e} \bmod(n)$）（$r^{e} \bmod(n)$）＞を第三者機関のサーバ２に送信する。

【００４７】

これによりエスクロー機関は、買い手の銀行口座からエスクロー機関の銀行口座

への振込指示を行う。買い手の口座からエスクロー機関の口座への振込あるいは振替が行われたことが銀行からエスクロー機関に通知されると、エスクロー機関は、ライセンスキーを買い手に渡す。具体的には、第三者機関のサーバ２が、（Ｋｒ）mod(n)を利用者の端末装置１に送信する。これにより、買い手は、耐タンパデバイス１３を利用してコンテンツＣを再生できる。

【００４８】

コンテンツＣの再生を確認した買い手は、その旨をエスクロー機関に通知する。

【００４９】

買い手からの確認を受け取ったエスクロー機関は、エスクロー機関の銀行口座から売り手の銀行口座への振込指示を行う。エスクロー機関の銀行口座から売り手の銀行口座への振込あるいは振替が行われると、その旨が銀行から売り手に通知される

【００５０】

このように、「ブラインド署名」アルゴリズムによる電子署名の匿名化技術を、ライセンス用暗号鍵の匿名化に応用することにより、第三者機関や利用者に対してライセンスキーとしての暗号鍵Ｋを隠蔽しつつ、コンテントＣの復号化を可能にし得る。

【００５１】

従来のエスクロー機関に対応する信頼できる第三者機関を利用するが、本実施形態におけるこのような機関は、コンテントＣのライセンスキーである暗号鍵Ｋ自体を預かることはせずに、自己の公開鍵＜ｅ，ｎ＞の公開と、それに対応した秘密鍵ｄを使用した計算のサービスのみを行う。銀行などの決済機関による支払い完了通知などの方法によって利用者によるコンテント利用の正当性が証明されると、第三者機関は、その利用者が所有する耐タンパデバイス１３の中でのみ暗号鍵Ｋとして機能する固有のデータ（Ｋｒ）mod(n)を、自己の秘密鍵ｄを利用して計算して利用者に渡す。このライセンスキー（Ｋｒ）mod(n)は、当該利用者の耐タンパデバイス１３の中でのみ復号化手段として利用できるために、ライセンスを取得した利用者自身でも直接それを参照することや複製することができない

。このような方法によって、コンテントＣを復号化するための暗号鍵Ｋを入手した利用者がその暗号鍵Ｋを再配布することを不可能にできる。

【００５２】

また、各利用者が所有する耐タンパデバイス１３の内部において、ブラインド署名スキーマと同等の乱数を用いた匿名化攪乱を行い、匿名化した状態で第三者機関に復号化計算を行わせ、再び利用者の耐タンパデバイス１３の内部で乱数成分を除去することによって復号化を行うので、第三者機関に対しても暗号鍵Ｋを隠蔽できる。

【００５３】

また、エスクローサービスを行う第三者機関自身も、暗号鍵Ｋを管理する必要が無くなることによって、暗号鍵Ｋの管理のためのセキュリティコストが不要になり、設備や人員の管理などのコストをかけることなしにエスクローサービスを行うことが可能になる。さらに著作権者も、第三者機関に鍵寄託のためのコストを支払う必要がないために、コンテント配信のコストを削減することができる。

【００５４】

さらに、著作権者も、特定のメモリ装置を介することなく暗号化されたコンテントＫ（ｃ）を配信できるために、コンテント配信を使ったビジネスに参加するためのコストを削減できる。

【００５５】

また、耐タンパデバイス１３の長期記憶部２５に格納された秘密鍵ｄＵと対をなす公開鍵＜ｅＵ，ｎＵ＞を、信頼できる認証機関５が本人確認を行った上で公開鍵証明書などの方法で安全に配布するので、第三者機関が耐タンパデバイス１３の所有者を確認できる。

【００５６】

また、著作権者は、個人や小規模の事業者であっても、特殊な記憶装置や再生装置やそれを利用するためのライセンスコストを支払うことなく、運用コストの安い信頼できる第三者機関を利用するだけで、安全なコンテント配信ビジネスを行うことができる。

【００５７】

また、サーバを利用しない、携帯型電話装置や携帯端末などの端末システムから端末システムへの複製の連鎖を利用したＰ２Ｐと呼ばれる形態でのコンテント配信においても、耐タンパデバイス１３を利用することによってコンテントＣやライセンスキーとしての暗号鍵Ｋの不正な複製を防ぎ、かつ第三者機関を利用することによって安全な決済を行うことができる。

【００５８】

以上のことから、たとえば、Ｐ２Ｐコマースに代表される個人間の著作物の交換や小規模事業者のコンテント配信においても、コンテントＣの著作権保護を安全かつ低コストで実現できる。

【００５９】

なお、上記実施形態においては、コンテント配信を、著作権者の端末装置３から利用者の端末装置１への通信網４を利用した通信によって実現したが、暗号化されたコンテントＫ（ｃ）を記録した光ディスクなどの記録媒体を著作権者から利用者に配布することによりコンテント配信を実現してもよい。

【００６０】

また、上記実施形態においては、１つの第三者機関を用いてシステムを構築したが、第三者機関自身の秘密鍵の漏洩に基づく暗号鍵の発覚を確実に防止するために、複数の第三者機関を用いてシステムを構築し、複数の第三者機関から利用者に暗号鍵に関するデータを分散して送信するように構成してもよい。図５は、このような秘密分散の原理説明図である。すなわち、暗号鍵Ｋを秘密１と秘密２とに分割して暗号化することにより、いずれか一方では暗号鍵Ｋを復元できないが、両方が揃うことにより暗号鍵Ｋを復元できるようにするのである。

【００６１】

また、上記実施形態においては、暗号鍵Ｋを直接暗号化して利用者に配布したが、暗号鍵Ｋを複数に分割し、分割した情報を暗号化して利用者に配布してもよい。

【００６２】

たとえば、全ての利用者の耐タンパデバイス１３に、同一の公開鍵暗号の秘密鍵を格納しておき、それに対応する公開鍵を公開する。この共通の公開鍵を＜ｎ

ｃ，ｅｃ＞とし、秘密鍵をｄｃとする。そして、著作権者は、暗号鍵Ｋを秘密分散アルゴリズムを用いて２つの情報に分割する。この分割に際しては、たとえば次のような式を用いる。乱数Ｘ１，Ｘ２，Ａと素数Ｐに対して、Ｙ１＝Ｋ＋（Ａ・Ｘ１）mod(P)，Ｙ２＝Ｋ＋（Ａ・Ｘ２）mod(P)。この式を用いることにより、結果として、Ｋは＜Ｘ１，Ｙ１＞と＜Ｘ２，Ｙ２＞とに分割される。このうち、Ｙ１を利用者の耐タンパデバイス１３共通の公開鍵＜ｎｃ，ｅｃ＞で暗号化した$(Y1)^{ec}$ mod(nc)と、Ｙ２を第三者機関の公開鍵＜ｎ，ｅ＞で暗号化した$(Y2)^{e}$ mod(n)とを演算する。そして、暗号化されたコンテントとともに、$K^{e}$ mod(n)の代わりに、$(Y1)^{ec}$ mod(nc)，$(Y2)^{e}$ mod(n)，Ｘ１，Ｘ２，Ｐを配布する。配布を受けた利用者側では、$(Y2)^{e}$ mod(n)を耐タンパデバイス１３の内部で乱数成分で匿名化したうえで第三者機関のサーバ２に送信する。第三者機関のサーバ２から復号結果を受信した利用者は、耐タンパデバイス１３の内部で乱数成分を除去し、Ｙ２を得る。また、耐タンパデバイス１３の内部で秘密鍵ｄｃを用いて$(Y1)^{ec}$ mod(nc)を復号化し、Ｙ１を得る。そして、耐タンパデバイス１３の内部で、＜Ｘ１，Ｙ１＞，＜Ｘ２，Ｙ２＞，Ｐを用いてＫ＝Ｙ１－（（Ｙ１－Ｙ２）／（Ｘ１－Ｘ２））mod(P)を演算し、暗号鍵Ｋを得る。

【００６３】

このようにすれば、利用者が耐タンパデバイス１３を利用せずに、直接的に$K^{e}$ mod(n)を第三者機関のサーバ２に送信して復号化を要求し、乱数成分の無いＫを直接得るという行為を、確実に防止できる。しかも、第三者機関が、コンテントとともに配信されている$K^{e}$ mod(n)を参照することによって、Ｋを復号化するという行為も、確実に防止できる。このような問題は、第三者機関が信頼でき、かつ第三者機関が適切な処置を行うという前提条件の下では防止可能ではあるが、上記のように暗号鍵Ｋを分割することによって、より本質的に解決できる。

【００６４】

また、上記実施形態においては、第三者機関から著作権者への公開鍵＜ｅ，ｎ＞の配布を通信網４を介して行うように構成したが、第三者機関から著作権者への公開鍵＜ｅ，ｎ＞の配布は如何なる方法を採用してもよい。

【００６５】

また、上記実施形態においては、暗号化方式としてＲＳＡ暗号を用いたが、ＲＳＡ暗号以外の暗号化方式を採用してもよいことはもちろんである。

【００６６】

（付記１）　配信者からコンテントの配信を受ける利用者のデータ処理装置と、

配信者と利用者との双方から信任された第三者機関のデータ処理装置と、

各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムであって、

前記利用者のデータ処理装置は、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置を備えており、

前記第三者機関のデータ処理装置は、前記配信者によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、前記耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを前記利用者のデータ処理装置に送信し、

前記耐タンパ装置は、前記第三者機関のデータ処理装置からの前記第１のデータを用いて、前記暗号化されたコンテントを復号化する構成としたことを特徴とする、コンテント配信システム。

【００６７】

（付記２）　コンテントを配信する配信者のデータ処理装置と、

コンテントの配信を受ける利用者のデータ処理装置と、

配信者と利用者との双方から信任された第三者機関のデータ処理装置と、

前記各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムであって、

前記配信者のデータ処理装置は、コンンツを暗号化して前記利用者のデータ処理装置に配信し、

前記利用者のデータ処理装置は、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置を備えており、

前記第三者機関のデータ処理装置は、前記暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、前記耐タンパ装置の内部でのみ暗号鍵

を求め得る第１のデータを前記利用者のデータ処理装置に送信し、

前記耐タンパ装置は、前記第三者機関のデータ処理装置からの前記第１のデータを用いて、前記暗号化されたコンテントを復号化する構成としたことを特徴とする、コンテント配信システム。

【００６８】

（付記３）　前記第三者機関のデータ処理装置は、公開鍵と秘密鍵とを記憶しており、前記配信者のデータ処理装置からの要求に応じて前記公開鍵を前記配信者のデータ処理装置に送信し、

前記配信者のデータ処理装置は、前記第三者機関のデータ処理装置から受信した前記公開鍵を用いて前記暗号鍵を暗号化し、その暗号化された暗号鍵を前記利用者のデータ処理装置に送信し、

前記利用者のデータ処理装置は、前記配信者のデータ処理装置から受信した前記暗号化された暗号鍵に基づく第２のデータを前記耐タンパ装置に生成させ、その第２のデータを前記第三者機関のデータ処理装置に送信し、

前記第三者機関のデータ処理装置は、前記利用者のデータ処理装置から受信した前記第２のデータと前記秘密鍵とを用いて前記第１のデータを生成する、付記２に記載のコンテント配信システム。

【００６９】

（付記４）　前記第三者機関は、複数存在し、

前記耐タンパ装置は、前記第２のデータを、前記暗号鍵が解読されないように秘密分散させて前記各第三者機関毎に各別に生成し、前記複数の第三者機関によって各別に生成された複数の前記第１のデータを用いて前記暗号鍵を解読し、その暗号鍵を用いて前記暗号化されたコンテントを復号化する、付記３に記載のコンテント配信システム。

【００７０】

（付記５）　前記耐タンパ装置は、前記暗号化された暗号鍵から前記第２のデータを生成するに際して、乱数成分を混入させ、前記第１のデータを用いて前記暗号化されたコンテントを復号化するに際して、前記第１のデータから前記乱数成分を除去する、付記３または４に記載のコンテント配信システム。

【００７１】

（付記６）　前記耐タンパ装置は、前記公開鍵に関する情報を、認証機関によるデジタル証明書の形式で記憶しており、かつ、前記認証機関により本人確認の上で各利用者に配布され、

前記第三者機関のデータ処理装置は、前記利用者のデータ処理装置から前記デジタル証明書の形式の前記公開鍵に関する情報を受信することにより、利用者の確認を行う、付記２ないし５のいずれかに記載のコンテント配信システム。

【００７２】

（付記７）　コンテントを配信する配信者のデータ処理装置と、前記コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、前記各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムにおいて、前記利用者のデータ処理装置に備えられ、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置であって、

前記第三者機関のデータ処理装置から受信した、前記配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵に関するデータを用いて、前記暗号鍵を解読する解読手段と、

前記解読手段によって解読された前記暗号鍵を用いて前記暗号化されたコンテントを復号化する復号化手段とを備えたことを特徴とする、耐タンパ装置。

【００７３】

（付記８）　コンテントを配信する配信者のデータ処理装置と、前記コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、前記各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムにおいて、前記第三者機関のデータ処理装置を実現するサーバであって、

前記配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、前記利用者のデータ処理装置に備えられた外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを生成するデータ生成手段と、

前記データ生成手段によって生成された前記第１のデータを前記通信網を介して前記利用者のデータ処理装置に送信するデータ送信手段とを備えたことを特徴とする、サーバ。

【００７４】

（付記９）　コンテントを配信する配信者のデータ処理装置と、前記コンテントの配信を受ける利用者のデータ処理装置と、配信者と利用者との双方から信任された第三者機関のデータ処理装置と、前記各データ処理装置を相互に通信可能に接続する通信網とを有するコンテント配信システムにおいて、前記第三者機関のデータ処理装置を動作させるためのコンピュータ・プログラムであって、

前記配信者のデータ処理装置によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、前記利用者のデータ処理装置に備えられた外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを生成するためのデータ生成プログラムと、

前記データ生成プログラムによって生成された前記第１のデータを前記通信網を介して前記利用者のデータ処理装置に送信するためのデータ送信プログラムとを含むことを特徴とする、コンピュータ・プログラム。

【００７５】

（付記１０）　配信者から暗号化されたコンテントの配信を受ける利用者のデータ処理装置と、

配信者と利用者との双方から信任された第三者機関のデータ処理装置と、

前記各データ処理装置を相互に通信可能に接続する通信網とを有するシステムにおいて実行されるコンテント配信方法であって、

前記利用者のデータ処理装置が、前記第三者機関のデータ処理装置に対して前記コンテントに対する支払い手続を指示するステップと、

前記第三者機関のデータ処理装置が、前記コンテントの対価について利用者の口座から第三者機関の口座への振替または振込が成功したときに、前記利用者のデータ処理装置でのみ暗号鍵を求め得る第１のデータを前記利用者のデータ処理装置に送信するステップと、

前記利用者のデータ処理装置が、前記第三者機関のデータ処理装置からの前記

第１のデータを用いて、前記暗号化されたコンテントを復号化するステップと、

を含むことを特徴とする、コンテント配信方法。

【００７６】

（付記１１）　前記利用者のデータ処理装置は、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置を備えており、

前記第１のデータを用いて前記暗号化されたコンテントを復号化する処理は、前記耐タンパ装置によって行われる、付記１０に記載のコンテント配信方法。

【００７７】

（付記１２）　前記第三者機関のデータ処理装置は、公開鍵と秘密鍵とを記憶しており、

前記利用者のデータ処理装置によって、配信者から配信されかつ前記公開鍵を用いて暗号化された暗号鍵に基づく第２のデータが生成されて前記第三者機関のデータ処理装置に送信され、

前記第三者機関のデータ処理装置によって、前記利用者のデータ処理装置から受信した前記第２のデータと前記秘密鍵とから前記第１のデータが生成される、付記１０または１１に記載のコンテント配信方法。

【００７８】

（付記１３）　前記利用者のデータ処理装置によって、前記暗号化された暗号鍵から前記第２のデータを生成するに際して、乱数成分が混入され、かつ、前記第１のデータを用いて前記暗号化されたコンテントを復号化するに際して、前記第１のデータから前記乱数成分が除去される、付記１２に記載のコンテント配信方法。

【００７９】

（付記１４）　前記耐タンパ装置によって、前記暗号化された暗号鍵から前記第２のデータが生成され、かつそのときに、乱数成分が混入され、

前記耐タンパ装置によって、前記第１のデータを用いて前記暗号化されたコンテントが復号化され、かつそのときに、前記第１のデータから前記乱数成分が除去される、付記１３に記載のコンテント配信方法。

【００８０】

（付記１５）　前記第三者機関のデータ処理装置が、前記利用者のデータ処理装置からのコンテンツを確認した旨の通知を受信することにより、コンテントの対価について第三者機関の口座から配信者の口座への振込手続を実行する、付記１０ないし１４のいずれかに記載のコンテント配信方法。

【００８１】

【発明の効果】

以上説明したように本発明によれば、第三者機関のデータ処理装置が、配信者によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを利用者のデータ処理装置に送信し、耐タンパ装置が、第三者機関のデータ処理装置からの第１のデータを用いて、暗号化されたコンテントを復号化するので、耐タンパ装置の外部からは暗号鍵を知ることができず、暗号鍵を確実に秘匿できる。

【図面の簡単な説明】

【図１】

本発明に係るコンテント配信システムの概略構成図である。

【図２】

利用者の端末装置の要部の構成図である。

【図３】

本発明に係るコンテント配信システムにおける配信プロトコルの説明図である。

【図４】

コンテンツ配信に伴う利用料金の決済の一例を説明する説明図である。

【図５】

秘密分散の原理説明図である。

【符号の説明】

１　利用者の端末装置

２　第三者機関のサーバ

３　著作権者の端末装置

４　通信網

５　認証機関

１１　コンテント再生処理部

１２　記憶部

１３　耐タンパデバイス

２１　演算部

２２　乱数生成部

２３　復号化部

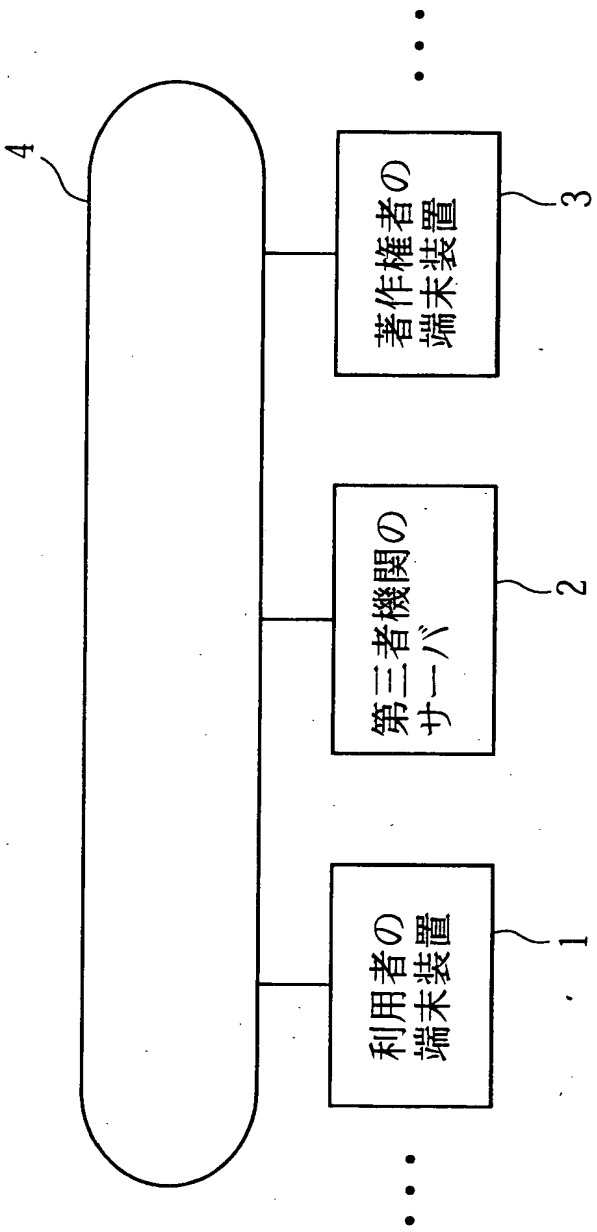
２４　一時記憶部

２５　長期記憶部

【書類名】　　図面

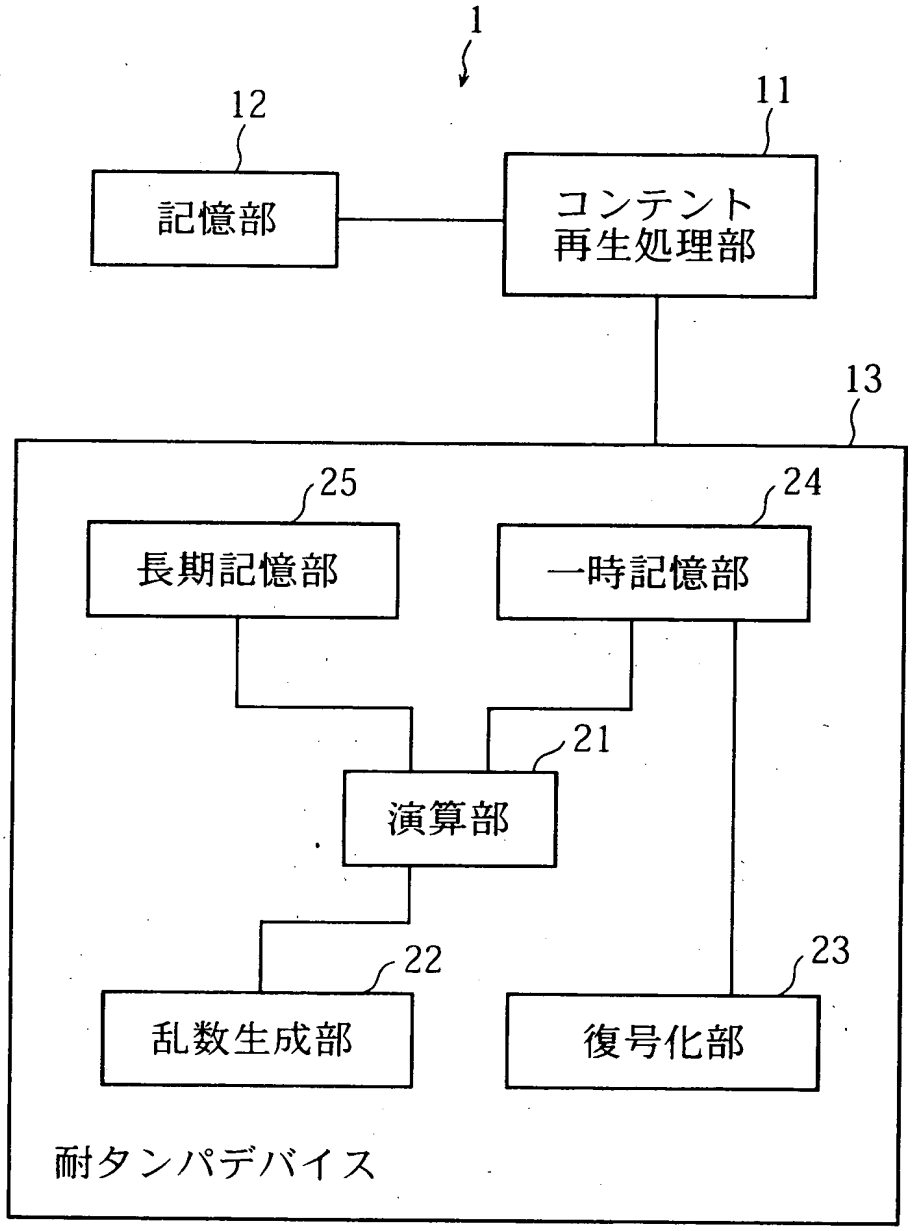
【図１】

本発明に係るコンテント配信システムの概略構成図



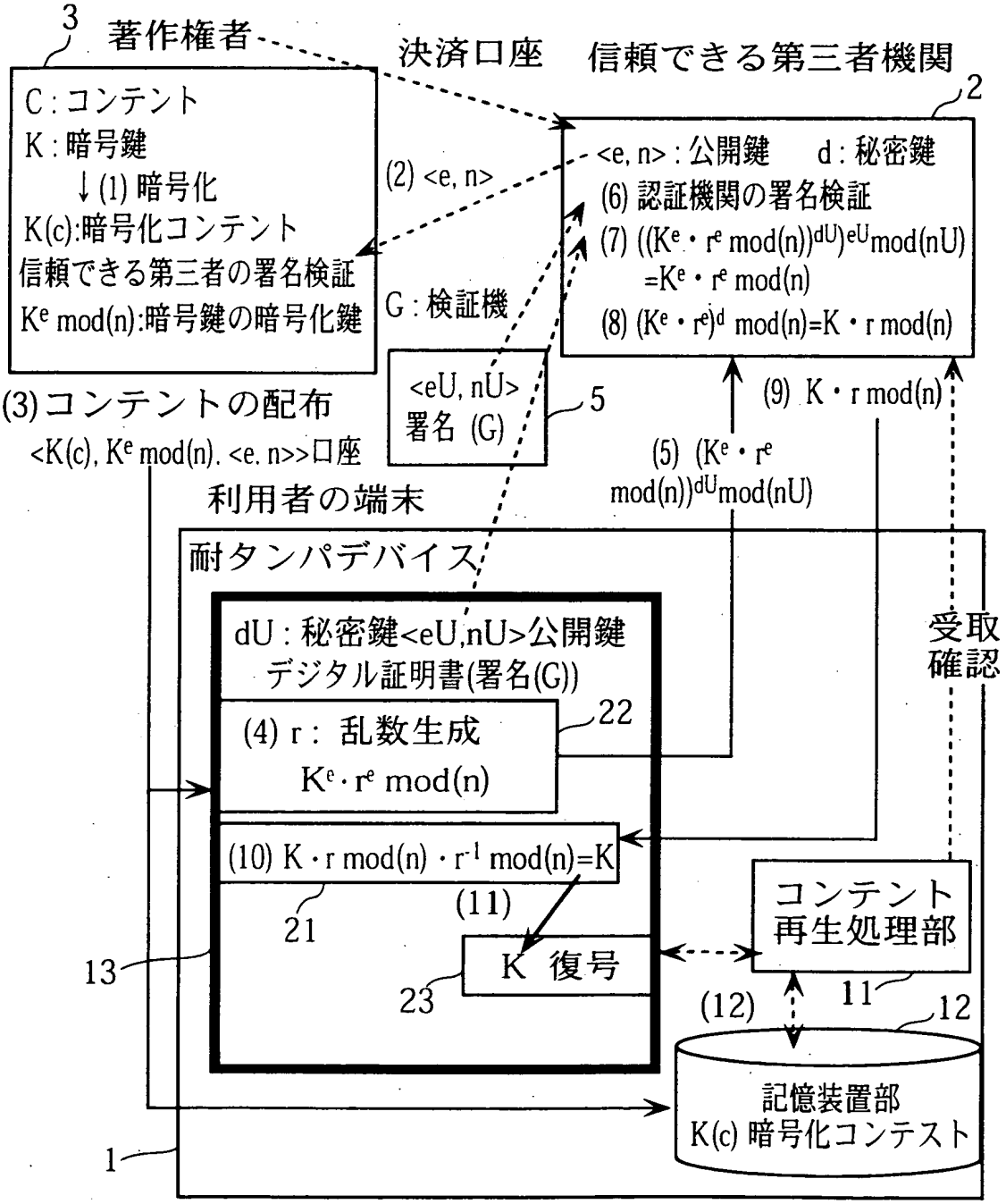
【図２】

利用者の端末装置の要部の構成図



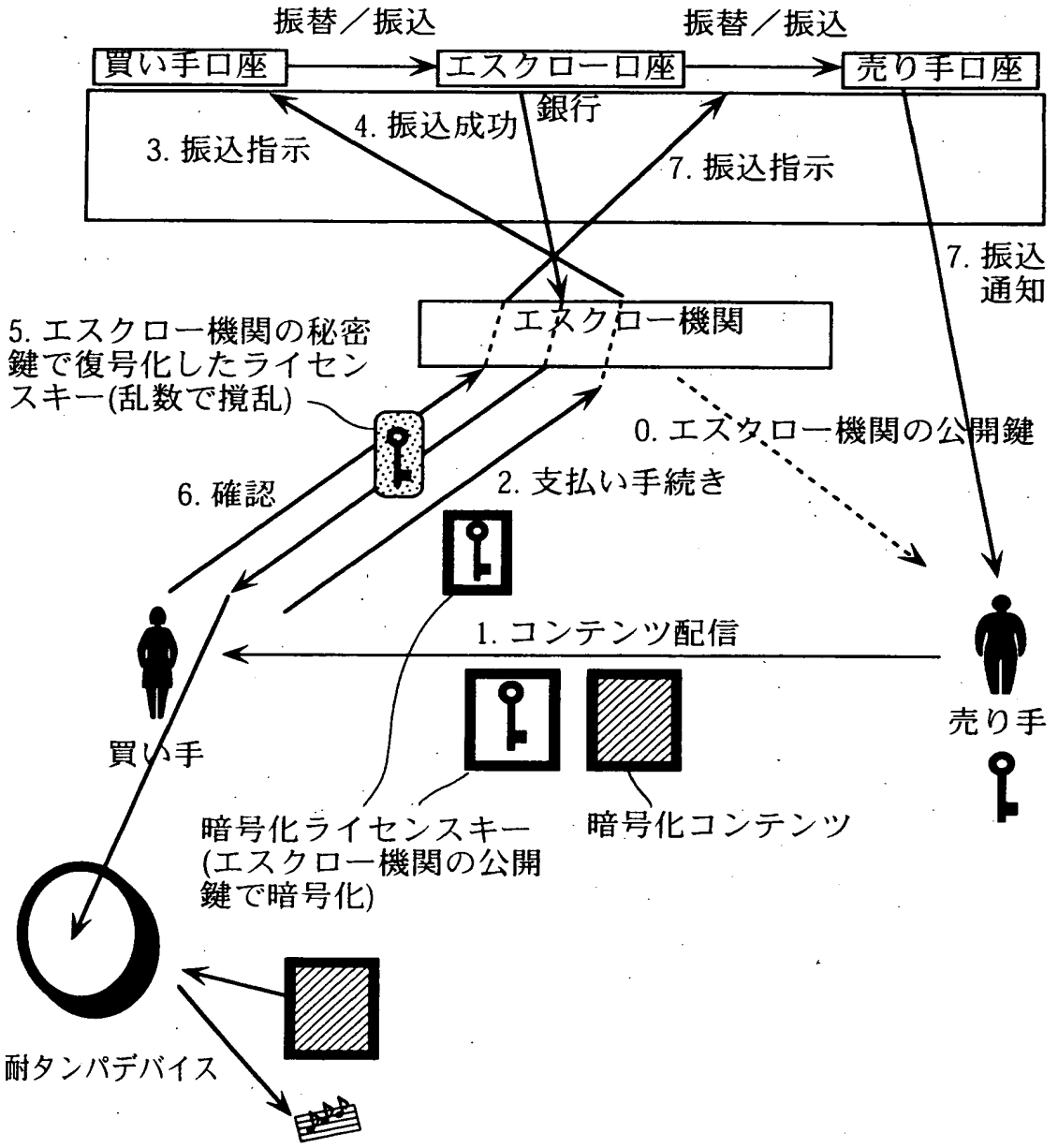
【図３】

本発明に係るコンテスト配信システムにおける
配信プロトコルの説明図



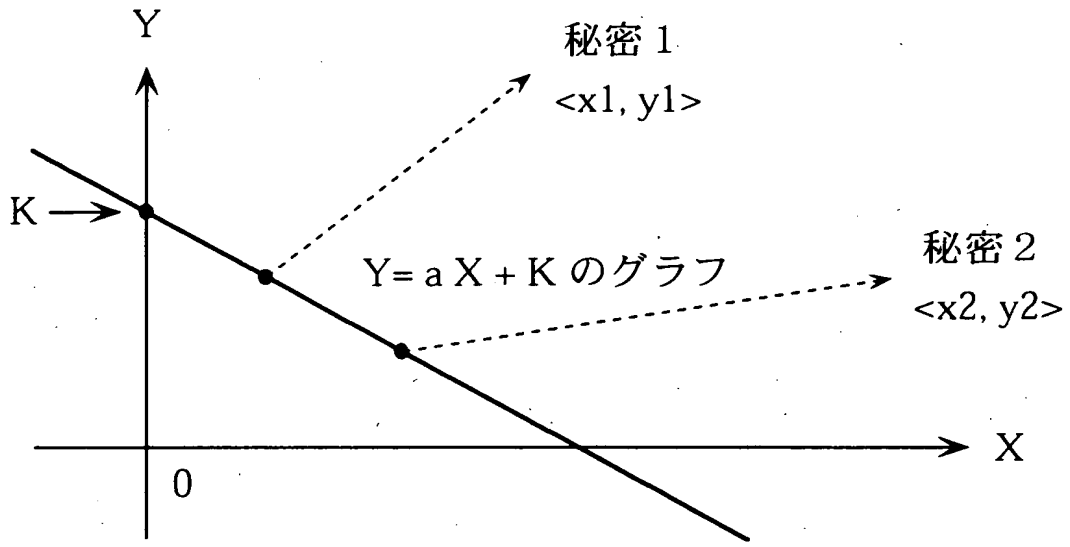
【図４】

コンテンツ配信に伴う利用料金の決済の一例を説明する説明図



【図５】

秘密分散の原理説明図



【書類名】　要約書

【要約】

【課題】　暗号鍵を確実に秘匿できるコンテント配信システムを提供する

【解決手段】　利用者の端末装置１は、外部から内容を知ることの不可能な耐タンパ性を有する耐タンパ装置を備えており、第三者機関のサーバ２は、著作権者の端末装置３によって暗号化されたコンテントを復号化するための暗号鍵に関するデータであって、耐タンパ装置の内部でのみ暗号鍵を求め得る第１のデータを利用者の端末装置１に送信し、耐タンパ装置は、第三者機関のサーバ２からの第１のデータを用いて、暗号化されたコンテントを復号化する構成とした。

【選択図】　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社